IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPELLANT :	Lundy LEWIS	CONFIRMATION NO.:	4279
SERIAL NUMBER :	09/578,156	EXAMINER:	Jeffrey R. Swearingen
FILING DATE :	May 23, 2000	ART UNIT:	2145
FOR :	METHOD AND APPARATUS FOR EVENT CORRELATION IN SERVICE LEVEL MANAGEMENT (SLM)		

Appellant's Brief on Appeal Under 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Further to the Notice of Appeal dated **August 30, 2007**, Appellant hereby submits this Appellant's Brief on Appeal pursuant to 37 C.F.R. § 41.37.

The Director is authorized to charge the fee for filing an Appeal Brief pursuant to 37 C.F.R. § 41.20(b)(2), as well as any additional fees that may be due, or credit any overpayment of same, to Deposit Account No. 033975 (**Ref. No. 019287-0317293**).

Appeal Brief Under 37 C.F.R. § 41.37

I. Real Party in Interest

By virtue of the assignment recorded at Reel 019047, Frame 0414, Computer Associates Think, Inc., the assignee of the present application, is the real party in interest.

II. Related Appeals and Interferences

The present application claims priority to U.S. Provisional Patent Application Serial No. 60/135,492, filed May 24, 1999, entitled "Method and Apparatus for Service Level Management." Appellant is also pursuing Appeals to the Board of Patent Appeals and Interferences in the following applications, each of which also claims priority to the above-identified U.S. Provisional Patent Application:

(1) U.S. Patent Application Serial No. 09/577,224, filed May 23, 2000, entitled "Method and Apparatus for Reactive and Deliberative Service Level Management (SLM)." Appellant's Request for Oral Hearing was filed July 17, 2007.

(2) U.S. Patent Application Serial No. 09/577,225, filed May 23, 2000, entitled "Service Level Management." Appellant's Brief on Appeal was filed September 20, 2007.

(3) U.S. Patent Application Serial No. 09/577,231, entitled "Method and Apparatus for Component to Service Mapping in Service Level Management (SLM)," filed May 23, 2000. Appellant's Brief on Appeal was filed August 29, 2007.

(4) U.S. Patent Application Serial No. 09/577,232, entitled "Method and Apparatus for Service Analysis in Service Level Management (SLM)," filed May 23, 2000. Appellant's Reply Brief and Request for Oral Hearing was filed October 15, 2007.

III. Status of Claims

Pending: Claims 1-6, 9-13, 15-18, 20-21, and 23-26 are pending.

Cancelled: Claims 7-8, 14, 19, and 22 are cancelled.

Rejected: Claims 1-6, 9-13, 15-18, 20-21, and 23-26 stand rejected.

Allowed: No claims have been allowed.

On Appeal: Claims 1-6, 9-13, 15-18, 20-21, and 23-26 are on appeal.

IV. Status of Amendments

No amendments to the claims have been filed subsequent to the Final Office Action dated April 30, 2007 (hereinafter "Final Action").

V. Summary of Claimed Subject Matter

According to various aspects of the invention, as recited in claims 1, 6, and 18, for example, service level management may be provided in a network that includes a plurality of network components (e.g., Specification at 18, line 25 – 19, line 3; and 20, lines 1-18). For example, a service having a state associated therewith (e.g., Specification at 20, lines 15-18) may operate on a subset of the plurality of network components (e.g., Specification at 20, lines 11-14).

Multiple monitoring agents may each monitor a respective aspect of operation of one or more of the network components (e.g., Specification at 21, line 21 – 23, line 10). In particular, each monitoring agent may detect events in the respective monitored aspect of operation (e.g., Specification at 47, line 18 – 48, line 2) and generate alarms as a function of the detected events (e.g., Specification at 48, lines 3-11). For instance, as recited in claims 6 and 18, a first monitoring agent may monitor a first aspect of operation of one or more of the network components (e.g., Specification at 47, lines 18-19), a second monitoring agent may monitor a second, different aspect of operation of one or more of the network components (e.g., Specification at 47, lines 19-20), and so on (e.g., Specification at 47, line 20 – 48, line 2).

Subsequently, an alarm correlation agent may receive the generated alarms from the monitoring agents (e.g., Specification at 48, lines 3-8). For example, as recited in claims 6 and 18, the alarm correlation agent may receive the generated alarms via an alarm repository (e.g., Specification at 48, lines 11-13). The alarm correlation agent may then determine a current state of the service based on the received alarms (e.g., Specification at 20, lines 11-30; 48, lines 19-28; and 60, lines 1-8). As such, when the current state of the service is undesirable, the

alarm correlation agent may issue one or more instructions to autonomously establish a desirable state of the service (e.g., Specification at 62, lines 16-27).

According to various aspects of the invention, as recited in claims 11, 13, and 21, for example, service level management may be provided in a network that includes a plurality of network components (e.g., Specification at 18, line 25 – 19, line 3; and 20, lines 1-18). For example, a service having a state associated therewith (e.g., Specification at 20, lines 15-18) may operate on a subset of the plurality of network components (e.g., Specification at 20, lines 11-14).

At least one monitoring agent may be disposed within the network to monitor an aspect of operation of one or more of the network components (e.g., Specification at 21, line 21 – 23, line 10). In particular, the monitoring agent detects events in the monitored aspect of operation (e.g., Specification at 47, line 18 – 48, line 2) and generates alarms as a function of the detected events (e.g., Specification at 48, lines 3-11).

Subsequently, an alarm correlation agent may receive the generated alarms from the monitoring agent (e.g., Specification at 48, lines 3-8). The alarm correlation agent can then determine a current state of the service by analyzing the received alarms (e.g., Specification at 20, lines 11-30; 48, lines 19-28; and 60, lines 1-8). Accordingly, when the current state of the service is undesirable, the alarm correlation agent may issue one or more instructions to autonomously establish a desirable state of the service (e.g., Specification at 62, lines 16-27).

According to various aspects of the invention, as recited in claims 23 and 26, for example, service level management may be provided in a network that includes a plurality of network components (e.g., Specification at 18, line 25 – 19, line 3; and 20, lines 1-18). For example, a service having a state associated therewith (e.g., Specification at 20, lines 15-18) may operate on a subset of the plurality of network components (e.g., Specification at 20, lines 11-14).

Multiple monitoring agents may each monitor a respective aspect of operation of one or more of the network components (e.g., Specification at 21, line 21 – 23, line 10). In particular, each monitoring agent detects events in the respective aspect of operation (e.g., Specification at 47, line 18 – 48, line 2) and generates alarms as a function of the detected

events (e.g., Specification at 48, lines 3-11). Furthermore, as recited in claim 26, various agents may communicate with one another to access events or alarms in other respective monitored aspects of operation (e.g., Specification at 42, line 24 – 43, line 14).

For example, claim 23 recites that each monitoring agent may include an alarm correlation agent that receives the generated alarms in addition to alarms generated by other monitoring agents (e.g., Specification at 42, line 24 – 43, line 14; and 48, lines 3-8). The generated alarms and the accessed events or alarms may then be analyzed (e.g., by the alarm correlation agent) to determine a current state of the service (e.g., Specification at 20, lines 11-30; 48, lines 19-28; and 60, lines 1-8). Accordingly, when the current state of the service is undesirable, one or more instructions may be issued (e.g., by a control agent that controls the respective monitored aspect of operation) to autonomously establish a desirable state of the service (e.g., Specification at 62, lines 16-27).

VI. Grounds of Rejection to be Reviewed on Appeal

(1) Claims 1, 6, 8, 11, 13-14, 18, 20-23, and 26 stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. Final Action at 3.

(2) Claims 1-6, 9-13, 15-18, and 20-26 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,336,139 to Feridun et al. ("Feridun"). Final Action at 3-5.

*****

Appellant notes that claim 1 also stands rejected under the judicially created doctrine of non-statutory obviousness-type double patenting as allegedly being unpatentable over claim 1 of U.S. Patent No. 6,430,712. Final Action at 5-6.

Appellant will consider filing a terminal disclaimer to overcome this rejection once otherwise patentable subject matter has been determined. Appellant further notes that the filing of a terminal disclaimer to obviate a rejection based on non-statutory double patenting is not an admission of the propriety of the rejection. See *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870 (Fed. Cir. 1991).

VII. Argument

A. *The Rejection Under § 112, Second Paragraph Must be Reversed Because the Claims are Clear and Definite.*

The Examiner has rejected claims 1, 6, 8, 11, 13-14, 18, 20-23, and 26 under § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. In particular, the Examiner alleges that the terms "a desirable state" and "when the current state of the service is undesirable" are "relative terms which render the claims indefinite." Final Action at 3. The rejection is improper, and must be reversed, for at least the reason that the claims are clear and definite, thus satisfying the statutory notice requirements of § 112, second paragraph.

Appellant initially notes that the statutory requirement of § 112, second paragraph serves the purpose of "reasonably appris[ing] those skilled in the art of the scope of the invention, § 112 demands no more." *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1378, 55 U.S.P.Q.2d 1279, 1283 (Fed. Cir. 2000). As such, Appellant is entitled to claim the invention with a *reasonable* degree of clarity and precision, as only insolubly ambiguous claims are to be considered indefinite. *See Metabolite Labs., Inc. v. Lab. Corp.*, 370 F.3d 1354, 1366, 71 U.S.P.Q.2d 1081, 1089 (Fed. Cir. 2004); *see also Xerox Corp. v. 3Com Corp.*, 458 F.3d 1310, 1323 (Fed. Cir. 2006). In the instant case, however, the Examiner alleges that the "terms 'desirable' and 'undesirable' are not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention." Final Action at 3. Appellant disagrees with the Examiner's assessment.

For example, § 112, second paragraph does not require claim terms to be specifically defined by the claims to be definite. Rather, the scope of claims in patent applications is to be determined *"not solely on the basis of the claim language*, but upon giving claims their broadest reasonable construction *'in light of the specification as it would be interpreted by one of ordinary skill in the art.'"* *Phillips v. AWH Corp.*, 415 F.3d 1303, 1316-17, 75 U.S.P.Q.2d 1321 (Fed. Cir. 2005) (emphasis added). Because "claim definiteness . . . depends on the skill level of

a person of ordinary skill in the art," it is important to consider that a "person of ordinary skill is also a person of ordinary creativity, not an automaton." *See AllVoice Computing P.L.C. v. Nuance Communications, Inc.*, 2007 U.S. App. LEXIS 23949 (Fed. Cir. 2007). Thus, applying the correct standard, the claim language at issue is clear and definite for at least the reason that the allegedly indefinite terms of "desirable" and "undesirable" states would have clear and readily discernable meanings to a person of ordinary skill in the art, especially when read in light of the Specification.

Specifically, the Specification describes, at length, that any given "service may have a predefined state," which may be "expressed as a range of parameter values," for example. Specification at 20, lines 19-21. Further, what constitutes a "desirable" or "undesirable" state may depend on the terms of any given service level agreement, which includes "a list of services and their corresponding service parameters and service levels." Specification at 24, lines 23-29. In any event, determining the state of a given service generally "involves finding a function or procedure that takes component parameters . . . as arguments and provides a value for an inferred, higher-level service parameter." Specification at 60, lines 2-8. As such, a determination can be made as to when "a service enters an undesirable state," which may result in one or more instructions being issued "until a desirable state . . . is achieved." Specification at 62, line 22 – 63, line 4.

Further, in response to previous arguments addressing these issues, the Examiner alleges that Appellant has "failed to point out where in the specification a desirable state was clearly described." Final Action at 2. The Examiner further alleges that the portions "of the specification as cited by [Appellant] do not provide the standard called for in the relevant inquiry." Final Action at 2. Appellant notes that the claim language clearly and unambiguously describe how a service is determined to be in a "desirable" or "undesirable" state. For example, claim 1 expressly provides that "the alarm correlation agent determines a current state of the service based on the received alarms." The "current state of the service" can thus be compared, for example, to "some value of a service parameter used to indicate acceptable service qualities" in order to determine whether the "current state" is "desirable" or "undesirable." *See, e.g.*, Specification at 20, line 11 – 21, line 8; and 60, line 1 – 65, line 7.

Accordingly, for at least the foregoing reasons, it is apparent that the claim language and the description provided in the Specification would "reasonably apprise those skilled in the art of the scope of the invention." *See Solomon v. Kimberly-Clark Corp.*, 216 F.3d at 1378, 55 U.S.P.Q.2d at 128. Thus, because the allegedly indefinite claim terms have a clear and discernable meaning, particularly when read in light of the Specification, the claims serve the statutory notice requirement of § 112, second paragraph. As such, the Examiner has failed to meet the burden for establishing indefiniteness under § 112, second paragraph. Thus, the rejection of claims 1, 6, 8, 11, 13-14, 18-, 20-23, and 26 under § 112, second paragraph is improper and must be reversed.

B. *The Rejection Under § 102 Must be Reversed Because the Examiner has Failed to Establish a* Prima Facie *Case of Anticipation.*

The Examiner has rejected claims 1-6, 9-13, 15-18, and 20-21, and 23-26 under § 102(e) as allegedly being anticipated by Feridun. The rejection is improper, and must be reversed, for at least the reason that the Examiner has failed to establish a *prima facie* case of anticipation, as Feridun fails to disclose each and every feature of the claimed invention.

More particularly, Feridun does not disclose at least the feature of "an alarm correlation agent that receives the generated alarms from the monitoring agents, wherein the alarm correlation agent determines a current state of the service based on the received alarms and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable," as recited in claim 1, for example. The Examiner alleges, however, that Feridun teaches this feature at col. 8, lines 15-45 and 55-61, and at col. 10, line 54 – col. 11, line 10. Final Action at 2-4. Appellant disagrees with the Examiner's assessment.

Feridun generally relates to correlating events by applying a set of correlation rules against an incoming event stream. For example, Feridun indicates that the correlation rules are "adapted to recognize a given pattern of one or more events indicative of a given condition." Feridun at col. 2, lines 46-48. Thus, when "a given event pattern is recognized . . . a given condition sought to be monitored has occurred, and the event correlator may then be used . . . to take a given action." Feridun at col. 2, lines 53-58. As such, Feridun relates, at best,

to an event correlator that uses software agents to analyze events to determine when given conditions (e.g., correlated events or alarms) have occurred.

In fact, the Examiner has characterized Feridun in the same manner as Appellant has discussed above. For example, the Examiner refers to the passage in which "Feridun looks for 'events' corresponding to a suspended attack on a network as part of a security and firewall system. One of ordinary skill in the art is well conversed in the fact that security systems commonly refer to events in the system detecting a warning or 'attack' as an 'alarm.'" Final Action at 2-3. As such, in the passages of Feridun indicating that "given software agents may generate events" to be "placed on the output queue" (e.g., col. 8, lines 29-31), the events placed in the output queue can generally be referred to correlated events or alarms.

In a similar respect, claim 1 recites, among other things, "multiple monitoring agents," each of which "detects events in the respective monitored aspect of operation and generates alarms as a function of the detected events." As such, Appellant's invention relates to "event correlation . . . divided into the concepts of event space and alarm space." Specification at 48, lines 1-2. Specifically, "the [monitoring] agents perform an event-to-alarm mapping function," and "[a]n alarm correlation agent . . . is provided to analyze the alarms." Specification at 48, lines 6-7. In this sense, the "alarms" are generated as a function of the "events," but the "alarms" and "events" exist at different levels of abstraction nonetheless. For example, claim 1 recites specific techniques for processing "alarms" or correlated events, which include determining "a current state of the service based on the received alarms," and in response thereto, issuing "instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable."

By contrast, Feridun only describes limited mechanisms for processing alarms or correlated events such as "issuing a control signal to control the software agent to perform some task, to deploy another software agent, or [to] effect some other action within or without the managed machine." Feridun at col. 2, lines 58-62. As such, Feridun only tangentially discusses subsequent processing that may include "forwarding one, some, or all of the correlated events to whomever is listening." Feridun at col. 12, lines 34-37. However, Feridun does not disclose how "whomever is listening" would actually process the correlated

events or alarms because Feridun only relates to correlation in an event space. Accordingly, for at least these reasons, Feridun does not disclose "an alarm correlation agent that receives the generated alarms from the monitoring agents, wherein the alarm correlation agent determines a current state of the service based on the received alarms and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable."

Accordingly, for at least the foregoing reasons, Feridun fails to disclose each and every feature recited in claim 1, including at least the feature of "an alarm correlation agent that receives the generated alarms from the monitoring agents, wherein the alarm correlation agent determines a current state of the service based on the received alarms and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable." The rejection is therefore improper and must be reversed.

Claims 6, 11, 13, 18, 21, 23, and 26 include features similar to those set forth in claim 1. Claims 2-5, 9-10, 12, 15-17, 20, and 24-25 depend from and add features to one of claims 1, 6, 11, 13, 18, and 23. Thus, the rejection of these claims is likewise improper and must be reversed for at least the same reasons.

VIII. Claims Appendix

The pending claims (i.e., claims 1-6, 9-13, 15-18, 20-21, and 23-26) are attached in **Appendix A.**

IX. Evidence Appendix

Appendix B: None.

X. Related Proceedings Appendix

Appendix C: None

Conclusion

For at least the foregoing reasons, Appellant respectfully submits that the claims are clear, definite, and allowable over the references relied upon by the Examiner. Therefore, reversal of the rejections is respectfully requested.

Date: **October 30, 2007**

Respectfully submitted,

By: _____

Rick A. Toering
Registration No. 43,195

PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. Box 10500
McLean, Virginia 22102
Main: 703-770-7900
Fax: 703-770-7901

Appendix A: Claims Appendix

1. **(Previously Presented)** A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the system comprising:

multiple monitoring agents that each monitor a respective aspect of operation of one or more of the network components, wherein each monitoring agent detects events in the respective monitored aspect of operation and generates alarms as a function of the detected events; and

an alarm correlation agent that receives the generated alarms from the monitoring agents, wherein the alarm correlation agent determines a current state of the service based on the received alarms and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

2. **(Original)** The system of claim 1, wherein the monitoring agents comprise at least one of:

an infrastructure monitoring agent to monitor operation of the network infrastructure;

a computer system monitoring agent to monitor operation of at least one computer system on the network;

a network traffic monitoring agent to monitor traffic on the network;

an application monitoring agent to monitor operation of at least one application operating on the network;

a trouble-ticketing agent to receive reports of problems by users with respect to operation of the network;

a response time monitoring agent to monitor a response time of a communication on the network;

a device monitoring agent to monitor operation of a device on the network; and

a multicomponent monitoring agent comprising an aggregate of any of the above monitoring agents.

3. (**Previously Presented**) The system of claim 1, wherein the monitoring agents and the alarm correlation agent comprise reasoning agents.

4. (**Original**) The system of claim 3, wherein the reasoning agents comprise one or more of:

a rule-based reasoning agent;

a model-based reasoning agent;

a state-transition graph based reasoning agent;

a code book based reasoning agent; and

a case-based reasoning agent.

5. (**Previously Presented**) The system of claim 1, comprising:

an alarm repository that receives the generated alarms from the monitoring agents, wherein the alarm correlation agent analyzes the alarms in the alarm repository.

6. (**Previously Presented**) A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the system comprising:

a first monitoring agent that monitors a first aspect of operation of one or more of the network components, wherein the first monitoring agent detects events in the first monitored aspect of operation and generates alarms as a function of the detected events;

a second monitoring agent that monitors a second aspect of operation of one or more of the network components, wherein the second aspect is different from the first aspect, and wherein the second monitoring agent detects events in the second monitored aspect of operation and generates alarms as a function of the detected events;

an alarm repository that receives the generated alarms from the first and second monitoring agents; and

an alarm correlation agent that analyzes at least the received alarms in the alarm repository, determines a current state of the service based on the analyzed alarms, and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

7-8. **(Cancelled)**

9. **(Previously Presented)** The system of claim 6, wherein the first and second monitoring agents comprise at least one of:

an infrastructure monitoring agent to monitor operation of the network infrastructure;

a computer system monitoring agent to monitor operation of at least one computer system on the network;

a network traffic monitoring agent to monitor traffic on the network;

an application monitoring agent to monitor operation of at least one application operating on the network;

a trouble-ticketing agent to receive reports of problems by users with respect to operation of the network;

a response time monitoring agent to monitor a response time of a communication on the network;

a device monitoring agent to monitor operation of a device on the network; and

a multicomponent monitoring agent comprising an aggregate of any of the above monitoring agents.

10. **(Previously Presented)** The system of claim 6, wherein the monitoring agents and the alarm correlation agent comprise reasoning agents, wherein the reasoning agents comprise one or more of:

a rule-based reasoning agent;

a model-based reasoning agent;

a state-transition graph based reasoning agent;

a code book based reasoning agent; and

a case-based reasoning agent.

11. (**Previously Presented**) A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components and at least one monitoring agent that monitors an aspect of operation of one or more of the network components, wherein the monitoring agent detects events in the monitored aspect of operation and generates alarms as a function of the detected events, and wherein a service operates on a subset of the plurality of network components, the service having a state, the system comprising:

an alarm correlation agent that receives the generated alarms from the monitoring agent, wherein the alarm correlation agent determines a current state of the service based on the received alarms and issues one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

12. (**Previously Presented**) The system of claim 11, wherein the alarm correlation agent comprises one or more of:

a rule-based reasoning agent;

a model-based reasoning agent;

a state-transition graph based reasoning agent;

a code book based reasoning agent; and

a case-based reasoning agent.

13. (**Previously Presented**) A computer-implemented method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

monitoring at least one aspect of operation of one or more of the network components;

detecting events in the monitored aspect of operation;

generating alarms as a function of the detected events;

analyzing the generated alarms to determine a current state of the service; and

issuing one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

14. **(Cancelled)**

15. **(Previously Presented)** The method according to claim 13, wherein the monitored aspects of operation include at least one of:

operation of the network infrastructure;

operation of at least one computer system on the network;

traffic on the network;

operation of at least one application operating on the network; and

operation of a trouble-ticketing agent that receives reports of problems by users with respect to operation of the network;

operation of a device on the network;

a response time of a communication on the network; and

an aggregate of any of the above aspects of operation.

16. **(Previously Presented)** The method of claim 13, wherein generating the alarms includes applying at least one of:

rule-based reasoning;

model-based reasoning;

state-transition graph based reasoning;

code book based reasoning; and

case-based reasoning.

17. (**Previously Presented**) The method of claim 13, wherein analyzing the generated alarms includes applying at least one of:

rule-based reasoning;

model-based reasoning;

state-transition graph based reasoning;

code book based reasoning; and

case-based reasoning.

18. (**Previously Presented**) A computer-implemented method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

monitoring a first aspect of operation of one or more of the network components;

detecting events in the first monitored aspect of operation;

generating a first set of alarms as a function of the detected events in the first monitored aspect of operation;

monitoring a second aspect of operation of one or more of the network components, wherein the second aspect is different from the first aspect;

detecting events in the second monitored aspect of operation;

generating a second set of alarms as a function of the detected events in the second monitored aspect of operation;

sending the generated first and second sets of alarms to an alarm repository;

analyzing at least the first and second generated sets of alarms in the alarm repository to determine a current state of the service; and

issuing one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

19. (**Cancelled**)

20. (**Previously Presented**) The method of claim 18, wherein the one or more issued instructions control an aspect of operation of one or more of the network components.

21. (**Previously Presented**) A computer readable medium having computer executable instructions recorded thereon, wherein the computer executable instructions are operable to direct a computer to perform a method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

monitoring at least one aspect of operation of one or more of the network and components;

detecting events in the monitored aspect of operation;

generating alarms as a function of the detected events;

analyzing the generated alarms to determine a current state of the service; and

issuing one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

22. (**Cancelled**)

23. (**Previously Presented**) A computer-implemented system for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of components, the service having a state, the system comprising:

multiple monitoring agents that each monitor a respective aspect of operation of one or more of the network components, wherein each monitoring agent detects events in the respective aspect of operation and generates alarms as a function of the detected events, each monitoring agent including:

an alarm correlation agent that receives the generated alarms in addition to alarms generated by other monitoring agents, wherein the alarm correlation agent determines a current state of the service based on the received alarms; and

a control agent controls the respective monitored aspect of operation, wherein the control agent issues one or more instructions regarding the controlled aspect of operation to autonomously establish a desirable state of the service when the current state of the service is undesirable.

24. **(Previously Presented)** The system of claim 23, wherein the monitoring agents comprise at least one of:

an infrastructure monitoring agent to monitor operation of the network infrastructure;

a computer system monitoring agent to monitor operation of at least one computer system on the network;

a network traffic monitoring agent to monitor traffic on the network;

an application monitoring agent to monitor operation of at least one application operating on the network;

a trouble-ticketing agent to receive reports of problems by users with respect to operation of the network;

a response time monitoring agent to monitor a response time of a communication on the network;

a device monitoring agent to monitor operation of a device on the network; and

a multicomponent monitoring agent comprising an aggregate of any of the above monitoring agents.

25. **(Previously Presented)** The system of claim 23, wherein the monitoring agents comprise reasoning agents, and wherein the reasoning agents comprise at least one of:

a rule-based reasoning agent;

a model-based reasoning agent;

a state-transition graph based reasoning agent;

a code book based reasoning agent; and

a case-based reasoning agent.

26. **(Previously Presented)** A computer readable medium having computer executable instructions recorded thereon, wherein the computer executable instructions are operable to direct each of a plurality of agents to perform a method for providing service level management in a network, wherein the network includes a plurality of network components, and wherein a service operates on a subset of the plurality of network components, the service having a state, the method comprising:

monitoring at least one respective aspect of operation of one or more of the network and components;

detecting events in the respective monitored aspect of operation;

generating alarms as a function of the detected events;

communicating with other agents to access events or alarms in other respective monitored aspects of operation;

analyzing at least the generated alarms and the accessed events or alarms to determine a current state of the service; and

issuing one or more instructions to autonomously establish a desirable state of the service when the current state of the service is undesirable.

Appendix B: Evidence Appendix

None.

Appendix C: Related Proceedings Appendix

None.